

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

ANDREW KASNETZ

§
§
§
§
§
§

Criminal No. **3:18-CR-345-L**

MEMORANDUM OPINION AND ORDER

Before the court is Defendant's Motion to Suppress ("Motion") (Doc. 145) and Supplemental Motion to Suppress Evidence ("Supplemental Motion") (Doc. 144), both of which were filed on October 22, 2021. After considering the motions, the Government's responses, the evidence, Superseding Indictment, and applicable law, the court **denies** both of Defendant's suppression motions (Docs. 144, 145).

I. Procedural and Factual Background

In October 2017, law enforcement conducted an online investigation concerning the sharing of child pornography on BitTorrent, a peer-to-peer file sharing software program that allows users to search for, download, and share information with other users on the BitTorrent network. During the investigation, Detective Chris DeLeon used Torrential Downpour software that was specifically developed for use by law enforcement to investigate the online distribution of child pornography through BitTorrent software file sharing. Through the use of Torrential Downpour to search publicly available BitTorrent network file indices, Detective DeLeon came to believe that Defendant Kasnetz's IP address was associated with the download of child pornography files. Based on this information, Detective DeLeon applied for a warrant on February 20, 2018, to search Defendant Kasnetz's residence and seize information and electronic devices that would tend to establish that: (1) such device or devices were used to search, solicit, access,

display, possess, or distribute child pornography; and (2) identify the persons who used, controlled, or owned the devices. On the same date, Judge Brandon Birmingham of the 292nd Judicial District Court of Dallas County, Texas issued a search warrant authorizing the requested search of his residence and seizure of electronic devices.

On July 11, 2018, Defendant Kasnetz was charged in a two-count Indictment of possessing and receiving child pornography, which was superseded on September 22, 2020 (Doc. 81). Count One of the Superseding Indictment charges Defendant Kasnetz with receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2) and alleges that he downloaded a video file containing child pornography on February 20, 2018. Count One further alleges that the offending video file depicts a minor child's mouth being penetrated by a penis and the penis ejaculating into the child's mouth.

Counts Two and Three of the Superseding Indictment charge Defendant Kasnetz with possessing material containing child pornography that depicts prepubescent minors in violation of 18 U.S.C. § 2252A(a)(5)(B). Counts Two and Three both charge Defendant with possessing material—a HP Envy desktop computer and a Samsung laptop computer—containing child pornography on February 20, 2018. Both counts allege that offending files include detailed descriptions of minors engaged in sexually explicit conduct.

In his suppression motions, Defendant Kasnetz contends that law enforcement's pre-warrant investigation amounted to an unconstitutional warrantless search of his computers in violation of his Fourth Amendment rights and expectation of privacy. Defendant Kasnetz contends that the February 20, 2018 search of his residence that was conducted by law enforcement pursuant to a warrant was also unconstitutional because it exceeded the scope of the warrant. Defendant

Kasnetz, therefore, argues that all evidence obtained by law enforcement during these pre-warrant and post-warrant searches should be suppressed.

II. Motion to Suppress Legal Standard

The Fourth Amendment of the United States Constitution grants “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” A search occurs for the purposes of the Fourth Amendment “when the government violates a subjective expectation of privacy that society recognizes as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 33 (2001). “[T]o claim the Fourth Amendment’s protection, a defendant must have ‘a legitimate expectation of privacy in the invaded place.’” *United States v. Iraheta*, 764 F.3d 455, 461 (5th Cir. 2014) (citation omitted). “The proponent of a motion to suppress has the burden of establishing that his . . . Fourth Amendment rights were violated by the challenged search or seizure.” *Id.* (quoting *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978) (citations omitted). “[I]f a defendant produces evidence that he was arrested or subject to search without a warrant, the burden shifts to the government to justify the warrantless search.” *United States v. Roch*, 5 F.3d 894, 897 (5th Cir. 1993) (quoting *United States v. de la Fuente*, 548 F.2d 528, 533 (5th Cir. 1977)). Even in situations in which the government may bear the ultimate burden of persuasion, “the defendant must first discharge his initial burden of producing some evidence on specific factual allegations sufficient to make a prima facie showing of illegality.” *Id.* at 534 (citation omitted).

III. Analysis

A. Validity of Pre-Warrant Investigation

Defendant contends that law enforcement’s use of Torrential Downpour software to connect to his alleged IP address between October 6, 2017, and November 2, 2017, for purposes of obtaining information for use in applying for a warrant constitutes the fruit of an illegal search

via “government-sponsored malware which ‘tags’ or trespasses on an individual’s personal computer or other device to determine what websites the users of these computers visit, what digital files they appear to possess, and what digital files they appear to download.” Def.’s Mot.

1. Defendant contends that this warrantless investigative conduct by law enforcement was an intrusion on his personal and private protected space (computers) that violated the Fourth Amendment because:

Upon information and belief, during its intrusion upon a suspect’s computer or device, Torrential Downpour installs a “GUID tag” or “Glob,” which is malware, into a suspect’s computer or device’s private space without a warrant.

Based upon this initial warrantless search, the police obtained subscriber information for the IP address involved, and associated it with [him].

Based on information and belief, the police then ran a query of its “Child Protection data system” (a government data base) and developed the opinion that the IP address was allegedly “in complete or partial possession of known or suspected child pornography files.”

Upon information and belief, the basis of the government’s information relating to alleged digital files available on or downloaded by a computer connected at Defendant’s alleged IP address represent the fruits of government-sponsored malware which “tags” or trespasses on individuals’ personal computers to determine what websites the users of these computers allegedly visit, what digital files they appear to possess, and what digital files they allegedly download.

...

Here, *assuming that* government officials accessed [his] home computer, they have invaded his zone of privacy by “tagging” his computer and trespassing upon it using government-sponsored malware.

His home computer is a protected space.

The government’s use of malware and subsequent intrusion into [his] personal electronic space (by means of “tagging”) is a “search.”

Def.’s Mot (Doc. 145) 3-4 (emphasis added).

In *United States v. Landry*, the Fifth Circuit reiterated that “[t]here is no reasonable expectation of privacy with respect to IP addresses, or images and information made publicly available in a shared folder on a peer-to-peer network. 729 F. App’x 345, 346-47 (5th Cir. 2018) (citing *United States v. Weast*, 811 F.3d 743, 747-48 (5th Cir. 2016)). In response to Defendant’s Supplemental Motion, the Government provided evidence establishing that the BitTorrent software alleged to have been used by Defendant Kasnetz to download child pornography is a peer-to-peer network software that makes IP addresses, images, and other information publicly available to other BitTorrent users. The Government’s evidence further establishes that only publicly available information was accessed during Detective DeLeon’s investigative efforts.

Defendant Kasnetz, on the other hand, has presented no factual allegations or evidence to the contrary. While he contends, *based on information and belief*, that law enforcement placed malware on his computer, no facts are alleged in his Supplemental Motion to support this conclusory assertion. Moreover, the Government provided evidence that neither BitTorrent nor Torrential Downpour has the capability to use or install malware, tags, or globally unique identifiers (“GUID”). Accordingly, Defendant Kasnetz has failed to establish a Fourth Amendment violation in his Supplemental Motion.

B. Validity of Search Conducted Pursuant to a Warrant

Defendant Kasnetz next contends that law enforcement exceeded the scope of the search permitted by the warrant issued by Judge Birmingham because the plain language of the warrant did not allow the police to search the electronic devices seized at any place other than his residence. Defendant Kasnetz acknowledges that Judge Birmingham adopted the verified facts in Detective DeLeon’s affidavit as supporting probable cause. He, nevertheless, points to the following

language in the warrant to support his contention that any search done by law enforcement was required to take place at his residence:

NOW, THEREFORE you are authorized and commanded to enter the suspected place and premises located at [address omitted] as described in said Affidavit. This is to include all buildings, structures, and vehicles within the curtilage of said premises as well as the persons of Andrew Kasnetz . . . and/or persons unknown who are associated with said premises. *At said* place you shall search for and, if same be found, seize and bring before me the property, evidence, and items described in said Affidavit.

Def.'s Ex. 1 (emphasis added by Def.). For this reason, Defendant Kasnetz contends that law enforcement exceeded the scope of the warrant when they removed his desktop and laptop computers from his residence and performed an off-site forensic analysis of his computers and other electronic devices without obtaining another search warrant. The court disagrees and determines that the language in the warrant does not support this argument by Defendant.

As correctly noted by the Government, Detective DeLeon's affidavit emphasized the importance of being able to remove all seized electronic devices from Defendant's residence for purposes of conducting a scientific forensic analysis of such devices at another location to avoid accidental loss of data. Further, the warrant issued by Judge Birmingham expressly incorporates this request by granting law enforcement "leave and authority to remove any such seized property from Dallas County if such removal is expressly authorized by the provisions of Texas Code of Criminal Procedure Article 18.10." *Id.* Texas Code Criminal Procedure Article 18.10, which is referenced in the warrant, provides that "nothing herein shall prevent the officer, or his department, from forwarding any item or items seized to a laboratory for scientific analysis." Accordingly, Defendant's Motion and this ground for suppression are without merit and fail to establish a violation of the Fourth Amendment.

IV. Evidentiary Hearing

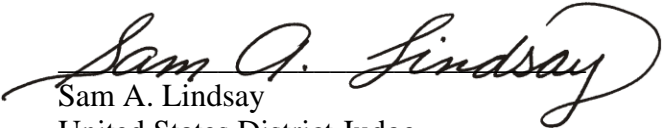
“Hearings on motions to suppress are not discovery proceedings, but are instead designed for the presentation of evidence in support of factual allegations which, if proven, would justify the relief sought.” *United States v. Harrelson*, 705 F.2d 733, 738 (5th Cir. 1983). For this reason, requests for evidentiary hearings are not granted as a matter of course; rather, they are only granted “when the defendant alleges sufficient facts which, if proven, would justify relief. *Id.* at 737; *United States v. Mergist*, 738 F.2d 645, 648 (5th Cir. 1984) (citations omitted). “Factual allegations set forth in the defendant’s motion, including any accompanying affidavits, must be “sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.” *Harrelson*, 705 F.2d at 737 (citations omitted). “General or conclusionary assertions, founded upon mere suspicion or conjecture, will not suffice.” *Id.*

As already noted, Defendant Kasnetz has not come forward with sufficiently specific factual allegations or evidence as required to warrant an evidentiary hearing on either of his motions. Instead, his contentions regarding the pre-warrant investigation are based on mere suspicion or conjecture, and his argument regarding law enforcement’s search of computers and other electronic devices is belied by the language in the warrant and Detective DeLeon’s supporting affidavit.

V. Conclusion

For the reasons explained, the court **denies** Defendant’s suppression motions (Docs. 144, 145) and **denies** his requests for an evidentiary hearing.

It is so ordered this 22nd day of March, 2022.


Sam A. Lindsay
United States District Judge